REMARKS

This is a full and timely response to the non-final Office Action of August 17, 2004. Reexamination, reconsideration, and allowance of the application and all presently pending claims are respectfully requested.

Upon entry of this First Response, claims 1-22 are pending in this application. Claims 1-3, 5, and 8-14 are directly amended herein, and claims 15-22 are newly added. It is believed that the foregoing amendments add no new matter to the present application.

Response to §102 Rejections

A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See, *e.g.*, *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

Claim 1

Claim 1 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Hayes* (U.S. Patent No. 6,339,826). Claim 1, as amended, reads as follows:

> 1. A computer system comprising:
> memory; and
> ***a security application configured to lock down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user***, said security application configured to store data indicative of said machine state in said memory, ***said security application configured to modify said machine state in response to a request for activating a new state of said security profile for said user, said security application configured to retrieve said data in response to a request for recovering said original state of said security profile and to modify said machine state based on said retrieved data thereby activating said original state of said security profile for said user***. (Emphasis added).

Applicants respectfully assert that *Hayes* fails to disclose at least the features of claim 1 highlighted hereinabove, and the 35 U.S.C. §102 rejection of claim 1, as amended, is therefore improper.

In rejecting claim 1, it is asserted in the Office Action that:

> "As per claims 1, 8, and 9, Hayes teaches: memory (Fig. 2, element 212); and a security application configured to lock down resources of said computer system (col. 19, lines 50-55) by modifying a machine state of said computer system in response to a request for activating a first security profile, said security application configured to store data indicative of said machine state in said memory (col. 17. lines 60-64) in response to said request for activating said first security profile (col. 7, lines 62-63), said security application configured to modify said machine state (col. 20, lines 1-5) in response to a request for activating a second security profile (col. 12, lines 34-46), said security application configured to retrieve said data in response to a request for recovering said first security profile and to modify said machine state based on said retrieved data (col. 7, lines 67-col. 8, lines 5)."

Thus, the Office Action appears to allege that the "user applet preferences" stored at the server 202 of *Hayes* constitute the "security profiles" recited in claim 1. Applicants observe, however, that each set of "user applet preferences" or, in other words, each alleged "security profile" appears to be configured for a particular user or set of users. Thus, when a context switch occurs, a new set of "user applet preferences" is retrieved and activated, but this new set of "user applet preferences" appears to be configured for a different user or set of users as compared to the previously activated set of "user applet preferences."

Claim 1 recites "modifying a machine state of said computer system in response to a request for activating an original state of a ***security profile for a user,***" further modifying the machine state in response to a request for activating a "new state" of the same "security profile" ***for the same "user,"*** and activating the "original state" in response to a "request for recovering said original state of said security profile." (Emphasis added). Noting that different sets of "user applet preferences" in *Hayes* appear to be configured for different users, as described above, Applicants assert that the performance of a context switch in *Hayes* does not anticipate at least the foregoing features of claim 1.

For at least the above reasons, Applicants respectfully assert that *Hayes* fails to disclose each features of claim 1, as amended, and the 35 U.S.C. §102 rejection of claim 1 should, therefore, be withdrawn.

Claims 2-4 and 15-19

Claims 2-4 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly being anticipated by *Hayes*. Further, claims 15-19 have been newly added via the amendments set forth herein. Applicants submit that the pending dependent claims 2-4 and 15-19 contain all features of their respective independent claim 1. Since claim 1 should be allowed, as argued hereinabove, pending dependent claims 2-4 and 15-19 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 5

Claim 5 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Hayes*. Claim 5, as amended, reads as follows:

> 5. A computer system, comprising:
> memory; and
> a security application defining a plurality of rules, ***said security application configured to enable a user to select a set of said rules to define an original state of a security profile for a user***, said security application configured to lock down said computer system by causing said computer system to enforce said selected set of rules in response to an activation request, said security application further configured to store data indicative of said original state of said security profile, ***said security application configured to change said security profile for said user from said original state to a new state*** by changing which of said plurality of rules are enforced by said computer system based on inputs to said computer system, said security application configured to retrieve said data in response to a user request and to automatically identify said set of rules based on said retrieved data, ***said security application further configured to return said security profile for said user to said original state thereby causing said computer system to enforce said identified rules in response to said user request***. (Emphasis added).

For at least the reasons set forth hereinabove in the arguments for allowance of claim 1, Applicants respectfully submit that *Hayes* fails to disclose at least the features of claim 5 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 5 should be withdrawn.

Claims 6 and 7

Claims 6 and 7 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly being anticipated by *Hayes*. Applicants submit that the pending dependent claims 6 and 7 contain all features of their respective independent claim 5. Since claim 5 should be allowed, as argued hereinabove, pending dependent claims 6 and 7 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 8

Claim 8 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Hayes*. Claim 8, as amended, reads as follows:

> 8. A computer system comprising:
> means for storing data; and
> ***means for locking down resources of said computer system by modifying a machine state of said computer system in response to a request for activating an original state of a security profile for a user***, said locking down means including a means for storing security profile data indicative of said machine state in said memory in response to said request for activating said original state of said security profile, ***said locking down means including a means for modifying said machine state in response to a request for activating a new state of said security profile for said user, said locking down means including a means for retrieving said security profile data in response to a request for recovering said original state of said security profile and for modifying said machine state based on said retrieved data thereby activating said original state of said security profile for said user***. (Emphasis added).

For at least the reasons set forth hereinabove in the arguments for allowance of claim 1, Applicants respectfully submit that *Hayes* fails to disclose at least the features of claim 8 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 8 should be withdrawn.

Claim 9

Claim 9 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Hayes*. Claim 9, as amended, reads as follows:

> 9. A method for locking down resources of a computer system, comprising:
> ***receiving a request for activating a an original state of a security profile for a user;***
> ***modifying a machine state of said computer system in response to said request for activating said original state of said security profile;***
> storing data indicative of said machine state;
> ***modifying said machine state in response to a request for activating a new state of said security profile for said user;***
> retrieving said data in response to a request for recovering said original state of said security profile; and
> ***modifying said machine state based on said retrieved data in response to said request for recovering said first security profile.*** (Emphasis added).

For at least the reasons set forth hereinabove in the arguments for allowance of claim 1, Applicants respectfully submit that *Hayes* fails to disclose at least the features of claim 9 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 9 should be withdrawn.

Claims 10-12, 20, and 21

Claims 10-12 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly being anticipated by *Hayes*. Further, claims 20 and 21 have been newly added via the amendments set forth herein. Applicants submit that the pending dependent claims 10-12, 20, and 21 contain all features of their respective independent claim 9. Since claim 9 should be allowed, as argued

hereinabove, pending dependent claims 10-12, 20, and 21 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 13

Claim 13 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Hayes*. Claim 13, as amended, reads as follows:

> 13. A method for locking down resources of a computer system, comprising:
> defining a plurality of rules for locking down said computer system;
> receiving an input from a user of said computer system;
> selecting a set of said rules based on said input;
> causing said computer system to enforce said selected set of rules in response to an activation request;
> storing data identifying said selected set of rules in response to said activation request;
> changing which of said plurality of rules are enforced by said computer system;
> ***detecting an operational problem caused by said changing***;
> ***providing a request to change a security state of said computer system in response to said detecting***;
> retrieving said data in response to said request to change said security state;
> automatically identifying said selected set of rules based on said retrieved data; and
> ***causing said computer system to enforce said selected set of rules in response to said request to change said security state***. (Emphasis added).

Applicants respectfully assert that *Hayes* fails to disclose at least the features of claim 13 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 13, as amended, is improper.

As set forth above in the arguments for allowance of pending claim 1, it is apparently alleged in the Office Action that *Hayes* discloses switching to different alleged "security profiles" when a context switch is performed. However, there is nothing in *Hayes* to indicate that a context switch is performed in response to a detection of an "operational problem" or that any request for changing from one state of an alleged "security profile" to another is provided in response to an

"operational problem." Thus, Applicants respectfully assert that *Hayes* fails to disclose at least the features of claim 13 highlighted above.

For at least the above reasons, Applicants respectfully assert that *Hayes* fails to disclose each features of claim 13, as amended, and the 35 U.S.C. §102 rejection of claim 13 should, therefore, be withdrawn.

Claim 14

Claim14 presently stands rejected in the Office Action under 35 U.S.C. §102 as allegedly being anticipated by *Hayes*. Applicants submit that the pending dependent claim 14 contains all features of its independent claim 13. Since claim 13 should be allowed, as argued hereinabove, pending dependent claim 14 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 22

Claim 22 has been newly added via the amendments set forth herein. Claim 22 presently reads as follows:

> 22. A computer system, comprising:
> memory; and
> a security application configured to define a security profile for controlling access to at least one resource of said computer system, said security application configured to activate an original state of said security profile and to store data indicative of said original state in said memory, said security application further configured to activate a new state of said security profile in response to a user request, said security application further configured to enable a user to undo an error in defining said new state by allowing said user to initiate activation of said original state based on said data.

Applicants respectively assert that the cited art fails to disclose or teach each feature of claim 22. Accordingly, claim 22 is allowable.

CONCLUSION

Applicants respectfully request that all outstanding objections and rejections be withdrawn and that this application and all presently pending claims be allowed to issue. If the Examiner has any questions or comments regarding Applicants' response, the Examiner is encouraged to telephone Applicants' undersigned counsel.

Respectfully submitted,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: 

Jon E. Holland
Reg. No. 41,077
(256) 704-3900 Ext. 103

Hewlett-Packard Development Company, L.P.
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400